

10/518973

CT/JP2004/005741

日 本 国 特 許 庁
JAPAN PATENT OFFICE

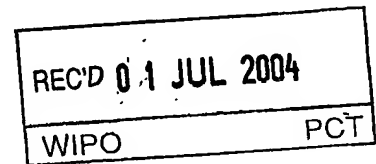
21. 4. 2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2003年 6月30日

出 願 番 号
Application Number: 特願2003-188141
[ST. 10/C]: [JP2003-188141]



出 願 人
Applicant(s): ソニー株式会社

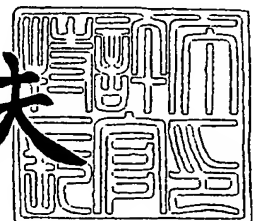
BEST AVAILABLE COPY

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年 6月 3日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 0390477820

【提出日】 平成15年 6月30日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 13/00

【発明の名称】 機器認証システム、端末機器、認証サーバ、サービスサーバ、端末機器方法、認証方法、端末機器プログラム、認証プログラム、サービスサーバプログラム、及び記憶媒体

【請求項の数】 20

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 小野 剛

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 三浦 貴之

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 鈴木 直志

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 宮田 耕自

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100096655

【弁理士】

【氏名又は名称】 川井 隆

【選任した代理人】

【識別番号】 100091225

【弁理士】

【氏名又は名称】 仲野 均

【先の出願に基づく優先権主張】

【出願番号】 特願2003-115755

【出願日】 平成15年 4月21日

【手数料の表示】

【予納台帳番号】 087218

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0114150

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 機器認証システム、端末機器、認証サーバ、サービスサーバ、端末機器方法、認証方法、端末機器プログラム、認証プログラム、サービスサーバプログラム、及び記憶媒体

【特許請求の範囲】

【請求項 1】 機器認証用の秘密情報を備えた端末機器と、前記秘密情報とを用いて前記端末機器の機器認証を行う認証サーバから構成された機器認証システムであって、

前記端末機器は、乱数を取得し、前記取得した乱数と前記秘密情報との組を一方方向性関数により変換して変換値を生成し、

前記認証サーバは、前記端末機器が取得した乱数、前記端末機器の秘密情報、及び前記端末機器が生成した変換値を取得し、

前記取得した乱数と秘密情報との組を前記端末機器が用いた一方方向性関数と同じ一方方向性関数により変換して変換値を生成し、

前記端末機器装置において生成した変換値と、前記認証サーバにおいて生成した変換値を比較することにより前記端末機器の機器認証を行うことを特徴とする機器認証システム。

【請求項 2】 請求項 1 の機器認証システムで機器認証を受ける端末機器であって、

認証サーバから、乱数と当該乱数を特定する乱数特定情報を受信する受信手段と、

前記受信した乱数と秘密情報の組を一方方向性関数により変換して変換値を生成する変換手段と、

前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信手段と、

を具備したことを特徴とする端末機器。

【請求項 3】 請求項 2 に記載の端末機器を機器認証する認証サーバであって、

乱数を取得する乱数取得手段と、

前記取得した乱数と、当該乱数を特定する乱数特定情報を端末機器に送信する送信手段と、

前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報を受信する受信手段と、

前記受信した乱数特定情報を用いて前記端末機器に送信した乱数を特定する乱数特定手段と、

前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定手段と、

前記特定した秘密情報と乱数の組を、前記端末機器が用い一方向性関数と同じ一方向性関数を用いて変換して変換値を生成する変換手段と、

前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証手段と、

を具備したことを特徴とする認証サーバ。

【請求項 4】 請求項 1 の機器認証システムは、認証サーバによる認証を経て前記端末機器にサービスを提供するサービスサーバを含み、

前記サービスサーバは、

乱数を取得する乱数取得手段と、

前記取得した乱数を端末機器に送信する乱数送信手段と、

前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報を受信する受信手段と、

前記端末機器に送信した乱数を特定する乱数特定手段と、

前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証情報を認証サーバに送信する認証情報送信手段と、

前記認証サーバから前記送信した認証情報による認証結果を受信する認証結果受信手段と、

を具備したことを特徴とするサービスサーバ。

【請求項 5】 請求項 4 に記載のサービスサーバからサービスの提供を受ける端末機器であって、

サービスサーバから乱数を受信する乱数受信手段と、

前記受信した乱数と、秘密情報の組を一方向性関数により変換して変換値を生成する変換手段と、

前記生成した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信手段と、

を具備したことを特徴とする端末機器。

【請求項 6】 請求項 4 に記載のサービスサーバがサービスを提供する際に、端末機器を機器認証する認証サーバであって、

サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を受信する受信手段と、

前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定手段と、

前記受信した乱数と前記特定した秘密情報との組を前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換手段と、

前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証手段と、

を具備したことを特徴とする認証サーバ。

【請求項 7】 請求項 1 の機器認証システムで機器認証を受ける端末機器で用いる端末機器方法であって、前記端末機器は、受信手段と、変換手段と、送信手段と、備えたコンピュータから構成されており、

認証サーバから、乱数と当該乱数を特定する乱数特定情報を前記受信手段で受信する受信ステップと、

前記受信した乱数と秘密情報の組を一方向性関数により前記変換手段で変換して変換値を生成する変換ステップと、

前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を前記送信手段で送信する送信ステップと、

から構成されたことを特徴とする端末機器方法。

【請求項 8】 請求項 2 に記載の端末機器を機器認証する認証サーバで用いる認証方法であって、前記認証サーバは、乱数取得手段と、送信手段と、受信

手段と、乱数特定手段と、秘密情報特定手段と、変換手段と、機器認証手段と、を備えたコンピュータから構成されており、

前記乱数取得手段で乱数を取得する乱数取得ステップと、

前記取得した乱数と、当該乱数を特定する乱数特定情報を前記送信手段で端末機器に送信する送信ステップと、

前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報を前記受信手段で受信する受信ステップと、

前記受信した乱数特定情報を用いて前記端末機器に送信した乱数を前記乱数特定手段で特定する乱数特定ステップと、

前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を前記秘密情報特定手段で特定する秘密情報特定ステップと、

前記特定した秘密情報と乱数の組を、前記変換手段で前記端末機器が用い一方方向性関数と同じ一方向性関数を用いて変換して変換値を生成する変換ステップと

前記受信した変換値と前記生成した変換値を用いて前記機器認証手段で前記端末機器を機器認証する機器認証ステップと、

から構成されたことを特徴とする認証方法。

【請求項 9】 請求項 4 に記載のサービスサーバで用いる認証方法であって、前記サービスサーバは、乱数取得手段と、乱数送信手段と、受信手段と、乱数特定手段と、認証情報送信手段と、認証結果受信手段と、を備えたコンピュータから構成されており、

前記乱数取得手段で乱数を取得する乱数取得ステップと、

前記取得した乱数を前記乱数送信手段で端末機器に送信する乱数送信ステップと、

前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報を前記受信手段で受信する受信ステップと、

前記端末機器に送信した乱数を前記乱数特定手段で特定する乱数特定ステップと、

前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証

情報を前記認証情報送信手段で認証サーバに送信する認証情報送信ステップと、
前記認証サーバから前記送信した認証情報による認証結果を前記認証結果受信手段で受信する認証結果受信ステップと、
から構成されたことを特徴とする認証方法。

【請求項 10】 請求項 4 に記載のサービスサーバからサービスの提供を受ける端末機器で用いる端末機器方法であって、前記端末機器は、乱数受信手段と、変換手段と、送信手段とを備えたコンピュータから構成されており、
前記乱数受信手段でサービスサーバから乱数を受信する乱数受信ステップと、
前記受信した乱数と、秘密情報の組を前記変換手段で一方向性関数により変換して変換値を生成する変換ステップと、
前記生成した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を前記送信手段で送信する送信ステップと、
から構成されたことを特徴とする端末機器方法。

【請求項 11】 請求項 4 に記載のサービスサーバがサービスを提供する際に、端末機器を機器認証する認証サーバが用いる認証方法であって、前記認証サーバは、受信手段と、秘密情報特定手段と、変換手段と、機器認証手段と、を備えたコンピュータから構成されており、

サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を前記受信手段で受信する受信ステップと、

前記秘密情報特定手段で、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定ステップと、

前記受信した乱数と前記特定した秘密情報との組を前記変換手段で前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換ステップと、

前記機器認証手段で、前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証ステップと、

から構成されたことを特徴とする認証方法。

【請求項 12】 請求項 1 の機器認証システムで機器認証を受けるコンピュータで構成された端末機器において、

認証サーバから、乱数と当該乱数を特定する乱数特定情報を受信する受信機能と、

前記受信した乱数と秘密情報の組を一方向性関数により変換して変換値を生成する変換機能と、

前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信機能と、

を実現する端末機器プログラム。

【請求項 13】 請求項 2 に記載の端末機器を機器認証するコンピュータで構成された認証サーバにおいて、

乱数を取得する乱数取得機能と、

前記取得した乱数と、当該乱数を特定する乱数特定情報を端末機器に送信する送信機能と、

前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報を受信する受信機能と、

前記受信した乱数特定情報を用いて前記端末機器に送信した乱数を特定する乱数特定機能と、

前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定機能と、

前記特定した秘密情報と乱数の組を、前記端末機器が用い一方向性関数と同じ一方向性関数を用いて変換して変換値を生成する変換機能と、

前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証機能と、

を実現する認証プログラム。

【請求項 14】 請求項 4 に記載のコンピュータで構成されたサービスサーバにおいて、

乱数を取得する乱数取得機能と、

前記取得した乱数を端末機器に送信する乱数送信機能と、

前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報を受信する受信機能と、

前記端末機器に送信した乱数を特定する乱数特定機能と、

前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証情報を認証サーバに送信する認証情報送信機能と、

前記認証サーバから前記送信した認証情報による認証結果を受信する認証結果受信機能と、

を実現するサービスサーバプログラム。

【請求項 15】 請求項 4 に記載のサービスサーバからサービスの提供を受けるコンピュータで構成された端末機器において、

サービスサーバから乱数を受信する乱数受信機能と、

前記受信した乱数と、秘密情報の組を一方向性関数により変換して変換値を生成する変換機能と、

前記生成した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信機能と、

を実現する端末機器プログラム。

【請求項 16】 請求項 4 に記載のサービスサーバがサービスを提供する際に、端末機器を機器認証するコンピュータで構成された認証サーバにおいて、

サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を受信する受信機能と、

前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定機能と、

前記受信した乱数と前記特定した秘密情報との組を前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換機能と、

前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証機能と、

を実現する認証プログラム。

【請求項 17】 請求項 12、又は請求項 15 に記載の端末機器プログラムを記憶したコンピュータが読み取り可能な記憶媒体。

【請求項 18】 請求項 13、又は請求項 16 に記載の認証プログラムを記憶したコンピュータが読み取り可能な記憶媒体。

【請求項 19】 請求項 14 に記載のサービスサーバプログラムを記憶したコンピュータが読み取り可能な記憶媒体。

【請求項 20】 請求項 1 の機器認証システムで機器認証を受ける端末機器であって、

認証サーバから、乱数と当該乱数を特定する乱数特定情報を受信する受信手段と、

前記受信した乱数と秘密情報の組を一方向性関数により変換して変換値を生成する変換手段と、

前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信手段と、

を具備し、

前記秘密情報と、前記変換手段は、端末機器に組み込まれた耐タンパ装置に格納されていることを特徴とする端末機器。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、認証システムなどに関し、特に、セキュリティ上重要な情報を所定のロジックで変換し、変換後の情報を用いて認証するものに関する。

【0002】

【従来の技術】

近年、CE (CE: Consumer Electronics) 機器の普及が広まりつつある。CE 機器とは、例えば、ビデオデッキ、ハードディスクレコーダ、ステレオ、テレビなどのオーディオビジュアル機器や、パーソナルコンピュータ、デジカメ、カムコーダ、PDA、ゲーム機、ホームルータ等の電子機器や、炊飯器、冷蔵庫などの家電製品や、その他の電子機器にコンピュータを内蔵させ、ネットワークを介したサービスを利用できるものである。

そして、CE 機器からサーバにアクセスしてコンテンツをダウンロードしたり、サービスを受けるなどし、ユーザはサーバが提供するサービスを利用することができる。

【0003】

サーバが提供するサービスには、CE機器全般に提供するものと、機器認証された特定のCE機器に提供するものがある。

サーバは、機器認証を要するサービスを提供する場合、そのCE機器を認証サーバで認証し、認証された場合にサービスを提供する。

このように、サービスサーバが端末機器にサービスを提供するものとして次の発明がある。

【0004】

【特許文献1】

特開 2002-342285

【0005】

この発明は、端末機器（携帯電話）から認証要求があった場合に、これを認証すると共に端末機器にワンタイムパスワードを発行して送信する。端末機器から情報の要求があった場合、端末機器から先のワンタイムパスワードを受信し、認証したのが確かにこの端末機器であることを確認するものである。

【0006】

図12は、従来のCE機器101の構成を示した図である。CE機器101は、機器IDやパスフレーズなどの認証に必要な認証情報を記憶していると共に、機器認証に関する処理を行う機器認証モジュール103と、機器認証モジュール103から認証情報を受け取り、通信経路を暗号化してこれを機器認証先105に送信する暗号化モジュール104を備えている。

【0007】

機器認証モジュール103は、暗号化モジュール104に認証情報を平文で渡すため、この認証情報が第三者に読み取られないように、機器認証モジュール103と暗号化モジュール104はスタティックリンクにて結合されている。

通信経路を暗号化するモジュールは、機器認証以外の用途で利用する場合も多いが、暗号化モジュール104は機器認証モジュール103とスタティックリンクされているため、CE機器101は、これとは別に機器認証以外の用途で使用する暗号化モジュールを用意している。

【0008】

【発明が解決しようとする課題】

このように、CE機器101では、同じ機能を有する2つの暗号化モジュールをCE機器101内のメモリに実装しなくてはならず、実質として機器認証モジュールの容量が多くなり、CE機器101の利用可能なメモリ領域を圧迫したり、あるいは機器認証機能の実装そのものが困難となる場合があった。

【0009】

そこで、本発明の目的は、端末機器内のメモリを有効利用することができる機器認証機能を実現できる端末機器認証システムなどを提供することである。

【0010】

【課題を解決するための手段】

機器認証用の秘密情報を備えた端末機器と、前記秘密情報とを用いて前記端末機器の機器認証を行う認証サーバから構成された機器認証システムであって、前記端末機器は、乱数を取得し、前記取得した乱数と前記秘密情報との組を一方向性関数により変換して変換値を生成し、前記認証サーバは、前記端末機器が取得した乱数、前記端末機器の秘密情報、及び前記端末機器が生成した変換値を取得し、前記取得した乱数と秘密情報との組を前記端末機器が用いた一方向性関数と同じ一方向性関数により変換して変換値を生成し、前記端末機器装置において生成した変換値と、前記認証サーバにおいて生成した変換値を比較することにより前記端末機器の機器認証を行うことを特徴とする機器認証システムを提供する（第1の構成）。

また、本発明は、第1の構成の機器認証システムで機器認証を受ける端末機器が、認証サーバから、乱数と当該乱数を特定する乱数特定情報を受信する受信手段と、前記受信した乱数と秘密情報の組を一方向性関数により変換して変換値を生成する変換手段と、前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信手段と、を具備するように構成することもできる（第2の構成）。

また、本発明は、第2の構成の端末機器を機器認証する認証サーバが、乱数を取得する乱数取得手段と、前記取得した乱数と、当該乱数を特定する乱数特定情

報を端末機器に送信する送信手段と、前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報を受信する受信手段と、前記受信した乱数特定情報を用いて前記端末機器に送信した乱数を特定する乱数特定手段と、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定手段と、前記特定した秘密情報と乱数の組を、前記端末機器が用い一方向性関数と同じ一方向性関数を用いて変換して変換値を生成する変換手段と、前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証手段と、を具備するように構成することもできる（第3の構成）。

また、本発明は、第1の構成の機器認証システムが、認証サーバによる認証を経て前記端末機器にサービスを提供するサービスサーバを含み、前記サービスサーバが、乱数を取得する乱数取得手段と、前記取得した乱数を端末機器に送信する乱数送信手段と、前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報を受信する受信手段と、前記端末機器に送信した乱数を特定する乱数特定手段と、前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証情報を認証サーバに送信する認証情報送信手段と、前記認証サーバから前記送信した認証情報による認証結果を受信する認証結果受信手段と、を具備するように構成することもできる（第4の構成）。

また、本発明は、第4の構成のサービスサーバからサービスの提供を受ける端末機器が、サービスサーバから乱数を受信する乱数受信手段と、前記受信した乱数と、秘密情報の組を一方向性関数により変換して変換値を生成する変換手段と、前記生成した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信手段と、を具備するように構成することもできる（第5の構成）。

また、本発明は、第4の構成のサービスサーバがサービスを提供する際に、端末機器を機器認証する認証サーバが、サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を受信する受信手段と、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定手段と、前記受信した乱数と前記特定した秘密情報との組を前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換手段と、前記受信した変換

値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証手段と、を具備するように構成することもできる（第6の構成）。

また、本発明は、第1の構成の機器認証システムで機器認証を受ける端末機器で用いる端末機器方法であって、前記端末機器は、受信手段と、変換手段と、送信手段と、備えたコンピュータから構成されており、認証サーバから、乱数と当該乱数を特定する乱数特定情報を前記受信手段で受信する受信ステップと、

前記受信した乱数と秘密情報の組を一方向性関数により前記変換手段で変換して変換値を生成する変換ステップと、前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を前記送信手段で送信する送信ステップと、から構成された端末機器方法を提供する。

また、本発明は、第2の構成の端末機器を機器認証する認証サーバで用いる認証方法であって、前記認証サーバは、乱数取得手段と、送信手段と、受信手段と、乱数特定手段と、秘密情報特定手段と、変換手段と、機器認証手段と、を備えたコンピュータから構成されており、前記乱数取得手段で乱数を取得する乱数取得ステップと、前記取得した乱数と、当該乱数を特定する乱数特定情報を前記送信手段で端末機器に送信する送信ステップと、前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報を前記受信手段で受信する受信ステップと、前記受信した乱数特定情報を用いて前記端末機器に送信した乱数を前記乱数特定手段で特定する乱数特定ステップと、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を前記秘密情報特定手段で特定する秘密情報特定ステップと、前記特定した秘密情報と乱数の組を、前記変換手段で前記端末機器が用いる一方向性関数と同じ一方向性関数を用いて変換して変換値を生成する変換ステップと、前記受信した変換値と前記生成した変換値を用いて前記機器認証手段で前記端末機器を機器認証する機器認証ステップと、から構成された認証方法を提供する。

また、本発明は、第4の構成のサービスサーバで用いる認証方法であって、前記サービスサーバは、乱数取得手段と、乱数送信手段と、受信手段と、乱数特定手段と、認証情報送信手段と、認証結果受信手段と、を備えたコンピュータから

構成されており、前記乱数取得手段で乱数を取得する乱数取得ステップと、前記取得した乱数を前記乱数送信手段で端末機器に送信する乱数送信ステップと、前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報を前記受信手段で受信する受信ステップと、前記端末機器に送信した乱数を前記乱数特定手段で特定する乱数特定ステップと、前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証情報を前記認証情報送信手段で認証サーバに送信する認証情報送信ステップと、前記認証サーバから前記送信した認証情報による認証結果を前記認証結果受信手段で受信する認証結果受信ステップと、から構成された認証方法を提供する。

また、本発明は、第4の構成のサービスサーバからサービスの提供を受ける端末機器で用いる端末機器方法であって、前記端末機器は、乱数受信手段と、変換手段と、送信手段とを備えたコンピュータから構成されており、前記乱数受信手段でサービスサーバから乱数を受信する乱数受信ステップと、前記受信した乱数と、秘密情報の組を前記変換手段で一方向性関数により変換して変換値を生成する変換ステップと、前記生成した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を前記送信手段で送信する送信ステップと、から構成された端末機器方法を提供する。

また、本発明は、第4の構成のサービスサーバがサービスを提供する際に、端末機器を機器認証する認証サーバが用いる認証方法であって、前記認証サーバは、受信手段と、秘密情報特定手段と、変換手段と、機器認証手段と、を備えたコンピュータから構成されており、サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を前記受信手段で受信する受信ステップと、前記秘密情報特定手段で、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定ステップと、前記受信した乱数と前記特定した秘密情報との組を前記変換手段で前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換ステップと、前記機器認証手段で、前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証ステップと、から構成された認証方法を提供する。

また、本発明は、第1の構成の機器認証システムで機器認証を受けるコンピュ

ータで構成された端末機器において、認証サーバから、乱数と当該乱数を特定する乱数特定情報を受信する受信機能と、前記受信した乱数と秘密情報の組を一方方向性関数により変換して変換値を生成する変換機能と、前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信機能と、を実現する端末機器プログラムを提供する。

また、本発明は、第2の構成の端末機器を機器認証するコンピュータで構成された認証サーバにおいて、乱数を取得する乱数取得機能と、前記取得した乱数と、当該乱数を特定する乱数特定情報を端末機器に送信する送信機能と、前記端末機器から、変換値と、前記乱数特定情報と、秘密情報特定情報を受信する受信機能と、前記受信した乱数特定情報を用いて前記端末機器に送信した乱数を特定する乱数特定機能と、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定機能と、前記特定した秘密情報と乱数の組を、前記端末機器が用い一方方向性関数と同じ一方方向性関数を用いて変換して変換値を生成する変換機能と、前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証機能と、を実現する認証プログラムを提供する。

また、本発明は、第4の構成のコンピュータで構成されたサービスサーバにおいて、乱数を取得する乱数取得機能と、前記取得した乱数を端末機器に送信する乱数送信機能と、前記端末機器から、秘密情報を用いて生成した変換値と、秘密情報特定情報を受信する受信機能と、前記端末機器に送信した乱数を特定する乱数特定機能と、前記受信した変換値と、秘密情報特定情報と、前記特定した乱数から成る認証情報を認証サーバに送信する認証情報送信機能と、前記認証サーバから前記送信した認証情報による認証結果を受信する認証結果受信機能と、を実現するサービスサーバプログラムを提供する。

また、本発明は、第4の構成のサービスサーバからサービスの提供を受けるコンピュータで構成された端末機器において、サービスサーバから乱数を受信する乱数受信機能と、前記受信した乱数と、秘密情報の組を一方方向性関数により変換して変換値を生成する変換機能と、前記生成した変換値と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信機能と、を実現

する端末機器プログラムを提供する。

また、本発明は、第4の構成のサービスサーバがサービスを提供する際に、端末機器を機器認証するコンピュータで構成された認証サーバにおいて、サービスサーバから、変換値と、秘密情報特定情報と、乱数からなる認証情報を受信する受信機能と、前記受信した秘密情報特定情報を用いて前記端末機器の秘密情報を特定する秘密情報特定機能と、前記受信した乱数と前記特定した秘密情報との組を前記端末機器が用いたのと同じ一方向性関数を用いて変換して変換値を生成する変換機能と、前記受信した変換値と前記生成した変換値を用いて前記端末機器を機器認証する機器認証機能と、を実現する認証プログラムを提供する。

また、本発明は、上記各プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する。

また、本発明は、請求項1の機器認証システムで機器認証を受ける端末機器であって、認証サーバから、乱数と当該乱数を特定する乱数特定情報を受信する受信手段と、前記受信した乱数と秘密情報の組を一方向性関数により変換して変換値を生成する変換手段と、前記生成した変換値と、前記受信した乱数特定情報と、認証サーバにおいて前記秘密情報を特定するための秘密情報特定情報を送信する送信手段と、を具備し、前記秘密情報と、前記変換手段は、端末機器に組み込まれた耐タンパ装置に格納されていることを特徴とする端末機器を提供する。

【0011】

【発明の実施の形態】

以下、本発明の好適な実施の形態について、図を参照して詳細に説明する。

(1) 実施形態の概要

図2に示したように、機器認証モジュール7は、認証サーバ5からサーバ乱数とワンタイムIDを受信し、このサーバ乱数とパスフレーズを組み合わせでハッシュ化してダイジェストを生成する。そして、これを機器IDと共に暗号化モジュール8に渡す。暗号化モジュール8は、通信経路を暗号化し、ダイジェストと機器ID、及びワンタイムIDを認証サーバ5に送信する。

【0012】

認証サーバ5は、予め機器IDとCE機器3のパスフレーズを対応付けて記憶

している。また、先にCE機器3に送信したサーバ乱数とワンタイムIDを対応付けて記憶している。

認証サーバ5は、CE機器3から受信したワンタイムIDと機器IDを用いてパスフレーズと先に発生したサーバ乱数を特定する。そしてこれらを組み合わせ、CE機器3側のロジックと同じロジックでダイジェストを生成する。そして、生成したダイジェストとCE機器3から受信したダイジェストを照合し、両者が一致するか否かでCE機器3の認証を行う。

【0013】

このように、機器認証モジュール7は、暗号化モジュール8にパスフレーズを渡さずに、サーバ乱数とパスフレーズの組から生成したダイジェストを渡す。そのため、機器認証モジュール7から第三者によりダイジェストが読み取られたとしても第三者はダイジェストからパスフレーズを復元することはできない。

【0014】

更に、認証サーバ5は、機器認証の度に異なるサーバ乱数を生成するため、機器認証モジュール7が暗号化モジュール8に渡すダイジェストも機器認証ごとに異なり、例えばダイジェストが第三者に読み取られたとしてもこれを乱用されることはない。

また、機器認証の度に同じダイジェストを用いる第三者にこのダイジェストが漏れた場合、これを元に所謂リプレイ攻撃が行われる可能性があるが、CE機器3は、機器認証の度に異なるダイジェストを生成するのでリプレイ攻撃されることはない。

【0015】

(2) 実施形態の詳細

図1は、本実施の形態の機器認証システム1の構成を説明するための図である。

機器認証システム1は、CE機器3、サービスサーバ4、認証サーバ5がネットワークを介して通信可能に接続されている。

なお、図1ではCE機器3とサービスサーバ4が一台ずつ記載されているが、これは複数存在させることができる。

【0016】

C E 機器 3 は、機器 I D、パスフレーズなど機器認証に必要な認証情報を備えており（記憶装置 3 a に記憶してある、図 3 の記憶部 2 8 に対応）、これらの情報を用いて認証サーバ 5 で機器認証を受け、サービスサーバ 4 が提供するサービスを利用することができる。

なお、パスフレーズは、C E 機器 3 と認証サーバ 5 が機器認証のために共有する秘密情報を構成している。

【0017】

サービスサーバ 4 は、C E 機器 3 に、例えば、コンテンツを送信するなどサービスを提供するサーバである。サービスサーバ 4 が提供するサービスには機器認証を要するものと要しないものがある。C E 機器 3 が機器認証を要するサービスを要求した場合、サービスサーバ 4 は、認証サーバ 5 に機器認証を代行してもらう。

【0018】

サービスサーバ 4 は、サービスを提供する C E 機器 3 を登録してあり、サービスサーバ 4 に接続可能な各 C E 機器の機器情報（シリアルナンバなど）、保有者情報などを記憶装置 4 a に記憶している。これらの情報は、C E 機器 3 から認証結果を受信した際に、認証サーバ 5 に機器認証を受けた C E 機器 3 が本当にこの C E 機器 3 であるか確認するのに用いる。

【0019】

認証サーバ 5 は、サービスサーバ 4 に代わって C E 機器 3 の機器認証を代行するサーバである。

認証サーバ 5 は、乱数（以下、サーバ乱数と呼ぶことにする）を生成して C E 機器 3 に送信し、C E 機器 3 から機器 I D、及びサーバ乱数とパスフレーズから生成したダイジェストなどを受信し、C E 機器 3 の機器認証を行う。認証サーバ 5 は、認証ごとに毎回異なったサーバ乱数を生成する。

認証サーバ 5 は、乱数を発生させることによりこれを取得する乱数取得手段を備えているが、認証サーバ 5 は、他の装置が生成した乱数取得するように構成することもできる。

【0020】

認証サーバ5は、各CE機器3ごとにパスフレーズ、機器ID、機器情報、保有者情報などを記憶装置5aに記憶しているほか、サービスサーバ4がCE機器3にサービスを提供するサービスサイトのURL (Uniform Resource Locators) も記憶している。

このURLは、CE機器3が利用しようとしているサイトが適切なものか否かを判断するために、予めサービスサーバ4が取得して登録したものである。

【0021】

認証サーバ5は、CE機器3から機器IDを受信、この機器IDにひも付けられたパスフレーズを検索することにより、CE機器3のパスフレーズを取得する。このように、機器IDはCE機器3の秘密情報 (パスフレーズ) を特定する秘密情報特定情報を構成している。

【0022】

サービスサーバ4のほかに機器認証を行う認証サーバ5を設けたのは (従来はサービスサーバ4が機器認証も行っていた)、サービスサーバ4は一般の個人や任意の団体などが運営する場合も多く、認証情報をサービスサーバ4に提供した場合、提供した情報が悪用されてしまう可能性があるためである。

【0023】

このように、機器認証の代行を行う認証サーバ5を設けたシステムとしては未公開の文献 (特願2002-144896) で提案されているサービス提供システムがある。

このシステムでは、機器認証を機器認証サーバが一括して行い、サービスサーバは、機器認証サーバでの認証結果を受け取って、CE機器にサービスを提供するか否かを判断する。

このシステムでは、機器認証を行う場合にセキュリティ上重要な情報を機器認証サーバに送信するため、これらの情報をサービスサーバに提供する必要がない。

【0024】

図2は、CE機器3を構成する要素のうち、機器認証に関するものを説明する

ための図である。

C E 機器 3 は、機器認証モジュール 7 と暗号化モジュール 8 を備えている。機器認証モジュール 7 は、機器 I D やパスフレーズなど、機器認証に必要な認証情報を記憶している。また、機器認証モジュール 7 は、認証サーバ 5 からサーバ乱数の受信し、これとパスフレーズを組み合わせてハッシュ化し、ダイジェスト（ハッシュ値、あるいはダイジェストメッセージ）を生成することができる。

機器認証モジュール 7 は、認証情報として機器 I D とダイジェストを暗号化モジュール 8 に渡す。

【0025】

ここでハッシュ化とは、ハッシュ関数と呼ばれる関数を用いて電子文書から文字列（ダイジェスト）を生成する処理のことである。

同じ電子文書からは同じダイジェストが得られる。電子文書が一部でも変更されると、この文書のダイジェストは、変更前のものと異なる。また、ダイジェストから元の電子文書を復元することはできない。

【0026】

なお、ハッシュ関数は一方向性関数と呼ばれる関数の一種である。一方向性関数とは、変換元から変換値への変換は容易であるが、変換値から変換元への逆変換が困難な関数である。そして、ダイジェストは、変換元（パスフレーズとサーバ乱数の組）をハッシュ関数で変換した変換値となる。

このように、C E 機器 3 は、乱数（サーバ乱数）と秘密情報（パスフレーズ）の組を一方向性関数で変換し変換値（ダイジェスト）を取得する変換手段を備えている。

【0027】

暗号化モジュール 8 は、例えば、SSL (Secure Sockets Layer) などの暗号化技術を使って、通信経路を暗号化するモジュールである。暗号化モジュール 8 は、機器認証モジュール 7 から認証情報を受け取り、暗号化した通信経路を経由して認証サーバ 5 に認証情報を送信する。

【0028】

このように、C E 機器 3 では、機器認証モジュール 7 から出力されるパスフレ

ーズは、サーバ乱数と組にして生成されたダイジェストとなっている。そのため、機器認証モジュール 7 から暗号化モジュール 8 に渡される認証情報には、平文のパスフレーズが含まれておらず、認証情報が第三者に渡ったとしても、ダイジェストからパスフレーズを復元することはできない。更に、機器認証に使用するダイジェストは毎回変化するので、第三者がダイジェストを読み取ってもこれを乱用することはできない。そのため高いセキュリティを確保することができる。

【0029】

機器認証モジュール 7 と暗号化モジュール 8 は、ダイナミックリンクにより接続される。

即ち、暗号化モジュール 8 は、機器認証モジュール 7 が認証情報を認証サーバ 5 に送信する際に暗号化モジュール 8 に動的に接続される。

そのため、暗号化モジュール 8 は、機器認証モジュール 7 とは別の通信経路を暗号化する必要があるモジュールからも利用できる。

【0030】

その場合は、そのモジュールが暗号化した通信経路で情報を送信する場合に暗号化モジュール 8 が動的にそのモジュールに接続する。

このように、暗号化モジュール 8 は、複数のモジュールから共用することができる。CE 機器 3 のメモリ領域を節約することができる。

【0031】

図 3 は、CE 機器 3 のハードウェア的な構成の一例を示した図である。

CPU (Central Processing Unit) 21 は、ROM (Read Only Memory) 22 に記憶されているプログラム、または記憶部 28 から RAM (Random Access Memory) 23 にロードされたプログラムに従って各種の処理を実行する。

また、RAM 23 には、CPU 21 が各種の処理を実行する上で必要なデータなども適宜記憶されている。

【0032】

CPU 21、ROM 22、および RAM 23 は、バス 24 を介して相互に接続されている。このバス 24 には、入出力インターフェース 25 も接続されている

入出力インターフェース 25 には、キーボード、マウスなどよりなる入力部 26、CRT (Cathode-ray Tube)、LCD (Liquid Crystal Display) などよりなるディスプレイ、並びにスピーカなどによりなる出力部 27、ハードディスクなどにより構成される記憶部 28、モデム、ターミナルアダプタなどにより構成される通信部 29 が接続されている。通信部 29 は、ネットワークを介しての通信処理を行う。

【0033】

また、入出力インターフェース 25 には、必要に応じてドライブ 30 が接続され、磁気ディスク 41、光ディスク 42、光磁気ディスク 43、またはメモリカード 44 などが適宜装着され、それから読み出されたコンピュータプログラムが、必要に応じて記憶部 28 にインストールされる。

なお、認証サーバ 5、サービスサーバ 4 の構成は基本的に CE 機器 3 と同様であるので説明は省略する。

【0034】

図 4 は、CE 機器 3 が認証サーバ 5 から機器認証を受ける手順を説明するためのフローチャートである。

なお、CE 機器 3 は、認証サーバ 5 の公開鍵を備えており、認証サーバ 5 は対応する秘密鍵を備えているものとする。

また、CE 機器 3 と認証サーバ 5 は、フローチャート中の括弧で示した各手段を備えている。

【0035】

CE 機器 3 がサービスサーバ 4 で機器認証が必要なサービスにアクセスすると、サービスサーバ 4 が CE 機器 3 に機器認証トリガーを送信する (ステップ 40)。

この機器認証トリガーは、CE 機器 3 に機器認証動作を開始させるための情報であり、認証サーバ 5 の URL や、サービスサイトが要求する認証のバージョンなどの情報が含まれている。

なお、機器認証にはいくつかのバージョンが用意されており、バージョンによ

り利用できるサービスが異なる場合がある。

【0036】

CE機器3は、サービスサーバ4から認証トリガを受信する。

以下の、CE機器3と認証サーバ5の通信は、暗号化モジュール8で暗号化された通信経路を介して行われる。

CE機器3は、認証トリガに含まれる認証サーバ5のURLを用いて認証サーバ5に接続し、サーバ乱数の送信を要求する(ステップ2)。

また、このとき、CE機器3は、認証トリガに含まれているサービスサーバ4が要求するバージョンと、CE機器3が実装している機器認証のバージョンを認証サーバ5に送信する。

【0037】

認証サーバ5は、CE機器3からサーバ乱数の送信要求を受信し、サーバ乱数を発生させる(乱数取得手段)(ステップ20)。また、サービスサーバ4が要求しているバージョンとCE機器3のバージョンが一致しているか否かの確認も行う。

更に、認証サーバ5は、ワнтаイムID1を生成する。そして、サーバ乱数とワнтаイムID1をCE機器3に送信する(送信手段)(ステップ22)。

【0038】

なお、サービスサーバ4は後ほど別のワнтаイムIDを生成するが、これと区別するため、上記のワнтаイムIDをワнтаイムID1とし、後に生成するワнтаイムIDをワнтаイムID2とする。

【0039】

このワнтаイムID1は、CE機器3と認証サーバ5でセッションを維持するために使用される使い捨てのIDである。

認証サーバ5は、CE機器3からワнтаイムID1を受信することによりCE機器3と維持しているセッションを認識することができる。

ワнтаイムID1は、機器認証ごとに異なる値が発行されるので、高いセキュリティを確保することができる。

【0040】

また、認証サーバ5は、送信したサーバ乱数とワнтаイムID1をひも付けして記憶する。これにより、後にCE機器3からワнтаイムID1を受信することにより、CE機器3に送信したサーバ乱数を特定することができる。このように、ワнтаイムID1は、乱数特定情報を構成している。

【0041】

CE機器3は、認証サーバ5からサーバ乱数とワнтаイムID1を受信する（受信手段）。ついで、CE機器3は、共通鍵を生成してこれを認証サーバ5の公開鍵で暗号化する（ステップ4）。この情報は、CE機器3の接続先が確かに認証サーバ5であることを確認するために用いられる。

次に、CE機器3は、パスフレーズとサーバ乱数を組み合わせて所定のロジックでハッシュを取り、ダイジェストを生成する（変換手段）（ステップ6）。

【0042】

次に、CE機器3は、機器ID、生成したダイジェスト、認証サーバ5から受信したワнтаイムID1を認証サーバ5を送信する（送信手段）（ステップ8）。

また、これらの情報と共に、先に公開鍵で暗号化した共通鍵と、CE機器3がサービスを受けようとしているサービスサーバ4のサイトのURL（以下ターゲットURLと呼ぶ）、及び、共通鍵を取り出すための秘密鍵（認証サーバ5は、複数の秘密鍵を持っている）を識別する秘密鍵識別子も認証サーバ5に送信する。

【0043】

認証サーバ5は、これらの情報をCE機器3から受信して（受信手段）、まずワнтаイムID1の確認を行う（ステップ24）。ワнтаイムID1により、認証サーバ5は、先に生成したセッションの続きであることを認識することができる。

また、ワнтаイムID1にひも付けて置いたサーバ乱数を記憶装置から取得することによりサーバ乱数を特定する（乱数特定手段）。

また、機器IDからCE機器3のパスフレーズを特定する（秘密情報特定手段）。

【0044】

更に、認証サーバ5は、CE機器3から受信したターゲットURLが、予め認証サーバ5に登録されているターゲットURLかも確認する。

これにより、CE機器3の接続先のサービスサーバ4が正当なサービスサーバ4であることを確認することができる。

【0045】

次に、認証サーバ5は、先にCE機器3に送信したサーバ乱数と、CE機器3のパスフレーズから、CE機器3と同じロジックによりダイジェストを生成し（変換手段）、これと、CE機器3から受信したダイジェストを照合してCE機器3の認証を行う（機器認証手段）（ステップ26）。

認証サーバ5は、認証に成功するとワнтаイムID2を生成する（ステップ28）。ワнтаイムID2は、後ほどCE機器3が認証を受けたのが確かに認証サーバ5であることをサービスサーバ4が確認するのに使用される。

また、認証サーバ5は、機器認証を行ったバージョンも記憶しておく。

【0046】

次に、認証サーバ5は、公開鍵で暗号化された共通鍵を秘密鍵で復号化して取り出す。

そして、認証サーバ5は、ワнтаイムID2をハッシュ化し、ダイジェスト（以下、ID2ダイジェストと呼ぶ）を生成する。

次に、認証サーバ5は、ID2ダイジェストを先に復号化した共通鍵で暗号する（ステップ30）。

【0047】

次に、認証サーバ5は、暗号化したID2ダイジェストと、ワнтаイムID2を連結して共通鍵で暗号化し、これをCE機器3に送信する（ステップ32）。

ワнтаイムID2にID2ダイジェストを連結するのは、送信されてきたワнтаイムID2のダイジェストを生成して、ID2ダイジェストと比較することにより、ワнтаイムID2が改変されたか否かを確認するためである。

【0048】

CE機器3は、認証サーバ5から暗号化されたワнтаイムID2とID2ダイ

ジェストを受信し、共通鍵でこれらを復号化する（ステップ10）。

CE機器3は、ワнтаイムID2をハッシュ化してダイジェストを生成し、これをID2ダイジェストと比較してワнтаイムID2が改竄されていないか確認する。

CE機器3は、共通鍵でこれらの情報が復号化できたことから、認証サーバ5が共通鍵を取り出せた（即ち、秘密鍵を持っている）ことを確認することができる。即ち、CE機器3が機器認証を求めた相手先は確かに認証サーバ5であったことを確認することができる（ステップ12）。

また、ワнтаイムID2が発行されたことから、CE機器3が機器認証されたことを確認することができる。

【0049】

次に、CE機器3は、認証サーバ5から受信したワнтаイムID2をサービスサーバ4に送信することにより、CE機器3が認証サーバ5で認証されたことを通知する（ステップ14）。

サービスサーバ4は、CE機器3からワнтаイムID2を受信し、これを認証サーバ5に送信して確かに認証サーバ5が機器認証したことを確認する（ステップ34、ステップ42）。

サービスサーバ4は、認証サーバ5で機器認証結果を確認すると、CE機器3に対してサービスの提供を開始する（ステップ44）。

そして、CE機器3ではサービスの利用を開始する（ステップ16）。

【0050】

以上の手順により、認証サーバ5は、パスフレーズそのものではなく、パスフレーズとサーバ乱数から生成されるダイジェストによりダイジェスト認証を行うことができる。

また、CE機器3は、共通鍵を公開鍵で暗号化して認証サーバ5に送信し、認証サーバ5の秘密鍵で共通鍵が取り出されたことを確認することにより、認証先が確かに認証サーバ5であることを確認することができる。

更に、認証サーバ5は、ワнтаイムID2にID2ダイジェストを貼付してCE機器3に送信することにより、CE機器3は、ワнтаイムID2が改竄されて

いないことを確認することができる。

【0051】

図5は、ステップ26（図4）のダイジェスト認証処理の手順を説明するためのフローチャートである。

認証サーバ5は、CE機器3へサーバ乱数とワンタイムID1を送信する際に、これらに対応付けて記憶している。

認証サーバ5は、CE機器3から受信したワンタイムID1を用いてCE機器3に送信したサーバ乱数を検索する（ステップ52）。

また、認証サーバ5は、機器IDとパスフレーズを予め対応付けて記憶しており、CE機器3から受信した機器IDからCE機器3のパスフレーズを検索する（ステップ54）。

【0052】

次に、認証サーバ5は、検索したサーバ乱数とパスフレーズの組をCE機器3と同じロジックによりハッシュ化し、ダイジェストを生成する（ステップ56）。

次に、認証サーバ5は、生成したダイジェストと、CE機器3から受信したダイジェストを比較し、同一か否かを判断する（ステップ58）。

【0053】

ダイジェストが一致した場合（ステップ60；Y）、認証サーバ5は、機器認証が成功したことを認識する（ステップ62）。

ダイジェストが一致しなかった場合（ステップ60；N）、認証サーバ5は、CE機器3が認証されなかったものと認識する（ステップ64）。

【0054】

以上のように、認証サーバ5は、ワンタイムIDとサーバ乱数に対応付けて記憶しておき、更に機器IDとパスフレーズに対応付けて記憶しておくことにより、CE機器3と同じロジックでダイジェストを生成することができ、CE機器3を機器認証することができる。

【0055】

図6は、ステップ34、ステップ42（図4）において、サービスサーバ4が

認証サーバ5で認証結果を確認する手順を説明するためのフローチャートである。

以下、認証サーバ5とサービスサーバ4の通信は、SSLなどの技術により暗号化された通信経路を介して行われるものとする。

【0056】

まず、サービスサーバ4は、認証サーバ5にCE機器3から受信したワнтаイムID2を送信し、機器認証の結果を要求する(ステップ82)。この際に、サービスサーバ4は、認証サーバ5とのセッションを維持するためのチケットを発行し、これも認証サーバ5に送信する。

【0057】

サービスサーバ4と認証サーバ5との送受信はお互いの信頼性が高いため、セッションの度にワнтаイムIDを発行せず、同じIDを複数回繰り返して使用してもよい。このように複数回再利用できるIDをチケットと呼ぶことにする。

ワнтаイムIDの代わりにチケットを発行することにより、サービスサーバ4と認証サーバ5の負荷を、ワнтаイムIDを発行した場合より小さくすることができる。

【0058】

認証サーバ5は、ワнтаイムID2を受信し、このワнтаイムID2をキーとして、CE機器3に対して行った機器認証のバージョンを検索する。また、CE機器3の機器IDなどからCE機器3の機器情報も検索する。

機器情報としては、例えば、CE機器3の製品コードやシリアルナンバなどがある。

そして、これら検索した情報をサービスサーバ4に送信する(ステップ72)。

【0059】

サービスサーバ4は、バージョン情報と機器情報を認証サーバ5から受信し、サービスサーバ4で記憶しているこれらの情報と照合する。

更に、サービスサーバ4は、認証サーバ5にチケットを送信し、CE機器3の保有者情報を認証サーバ5に要求する(ステップ84)。

認証サーバ5は、これに応じてこのCE機器3の保有者情報を検索し、チケットと共にサービスサーバ4に送信する（ステップ74）。

【0060】

サービスサーバ4は、認証サーバ5から受信した保有者情報をサービスサーバ4が記憶している保有者情報と照合する。

このように、機器情報や保有者情報を確認することにより、サービスサーバ4は、認証サーバ5は、確かにCE機器3を機器認証したことを確認することができる。

そして、サービスサーバ4は、CE機器3に対してサービスの提供を開始する（ステップ86）。

【0061】

以上のように、サービスサーバ4と認証サーバ5との間の複数回の送受信において同じチケットが繰り返し用いられる。

また、サービスサーバ4は、別の機器認証に関する認証結果確認には別のチケットを発行する。

【0062】

図7は、CE機器3が認証先が確かに認証サーバ5であることを確認する別のシーケンスを説明するためのフローチャートである。

以下の手順では、CE機器3が乱数（以下クライアント乱数と呼ぶことにする）を発生させ、これにより認証サーバ5を確認する。

まず、CE機器3は、クライアント乱数を生成する（ステップ102）。

次に、CE機器3は、共通鍵を生成する（ステップ104）。

【0063】

CE機器3は、生成した共通鍵でクライアント乱数を暗号化する（ステップ106）。暗号化した後の情報を暗号化情報1と呼ぶことにする。

更に、CE機器3は、認証サーバ5の公開鍵で共通鍵を暗号化する（ステップ108）。暗号化した後の情報を暗号化情報2と呼ぶことにする。

そして、CE機器3は、暗号化情報1と暗号化情報2を認証サーバ5に送信する（ステップ110）。

なお、C E 機器 3 は、送信したクライアントを記憶しておく。

【0064】

認証サーバ 5 は、C E 機器 3 から暗号化情報 1 と暗号化情報 2 を受信し、まず、認証サーバ 5 の秘密鍵で暗号化情報 2 を復号化し、共通鍵とを取り出す（ステップ 122）。

次に、認証サーバ 5 は、取り出した共通鍵で暗号化情報 1 を復号化し、クライアント乱数を取り出す（ステップ 124）。

次に、認証サーバ 5 は、取り出したクライアント乱数のハッシュをとり、ダイジェストを生成する（ステップ 126）。

次に、認証サーバ 5 は、生成したダイジェストを共通鍵で暗号化し、C E 機器 3 に送信する（ステップ 128）。

【0065】

C E 機器 3 は、認証サーバ 5 から暗号化したダイジェストを受信し、これを共通鍵で復号化する（ステップ 112）。

更に、C E 機器 3 は、記憶しておいた乱数をハッシュ化し、ダイジェストを生成する（ステップ 114）。

そして、C E 機器 3 は、生成したダイジェストと、先に復号化したダイジェストを比較し、両者が一致することにより、接続先が確かに認証サーバ 5 であることを確認する（ステップ 116）。

【0066】

即ち、クライアント乱数のダイジェストが共通鍵で暗号化されて送られてきたということは、接続先が暗号化情報 2 を復号化することができたということであり、これは、接続先が秘密鍵を持っていたことを意味する。秘密鍵を持っているのは認証サーバ 5 であるので、これにより、接続先が認証サーバ 5 であることを確認することができる。

【0067】

図 8 は、機器認証を行う他の手順を説明するためのフローチャートである。

図 4 に示した手順では、C E 機器 3 から認証サーバ 5 にアクセスして機器認証を行ったが、この手順では、C E 機器からサービスサーバ 4 に認証情報を送信し

、サービスサーバ4がこの認証情報を用いて認証サーバ5にアクセスして機器認証を行う。

以下の手順で、CE機器3、サービスサーバ4、認証サーバ5の間の通信は、例えば、SSLなどの技術により暗号化した経路が用いられるものとする。

また、CE機器3、サービスサーバ4、認証サーバ5は、フローチャート中に括弧で示した各手段を備えている。

【0068】

まず、CE機器3がサービスサーバ4に対して機器認証を要するサービスの提供を要求する。

これに対し、サービスサーバ4は、CE機器3に対して機器認証トリガを送信する（ステップ142）。

CE機器3は、サービスサーバ4から機器認証トリガを受信するとサービスサーバ4に対してサーバ乱数の要求を送信する（ステップ132）。

【0069】

サービスサーバ4は、これを受信してサーバ乱数を生成し（乱数取得手段）（ステップ144）、CE機器3に送信する（乱数送信手段）（ステップ146）。サービスサーバ4は、このサーバ乱数を記憶しておく。

CE機器3は、サービスサーバ4からサーバ乱数を受信すると共に（乱数受信手段）、クライアント乱数を生成する（ステップ134）。

次にCE機器3は、サーバ乱数、クライアント乱数、及びパスフレーズを組み合わせてハッシュ化し、ダイジェストを生成する（変換手段）（ステップ136）。

【0070】

次に、CE機器3は、生成したダイジェストと、機器ID、クライアント乱数をサービスサーバ4に送信して機器認証を要求する（送信手段）（ステップ138）。

サービスサーバ4は、これらの認証情報を受信する（受信手段）（ステップ148）。

このように、サービスサーバ4がCE機器3から受信する認証情報には、サー

バ乱数が含まれていない。

サービスサーバ4は、CE機器3から受信した認証情報（ダイジェスト、機器ID、クライアント）にサーバ乱数を加えて新たな認証情報とし、これを認証サーバ5に送信して機器認証を要求する（認証情報送信手段）（ステップ150）。

【0071】

ここでは、サービスサーバ4は、CE機器3とセッションを維持しているため、先に記憶したサーバ乱数がこのCE機器3に送ったサーバ乱数であることを認識することができる（乱数特定手段）。そこで、このサーバ乱数を認証情報に加えるのである。また、図4の手順と同様にしてワンタイムIDを発行することにより、CE機器3に送信したサーバ乱数を特定するように構成することもできる。

【0072】

このように、CE機器3から送られてきた認証情報に先に送信したサーバ乱数を付加するように構成することにより、認証トリガを送信したサービスサーバ4と認証情報を受信したサービスサーバ4が同一のサーバであることを確かめることができる。

【0073】

認証サーバ5は、サービスサーバ4から認証情報を受信し（受信手段）、CE機器3の機器認証を行う（ステップ162）。

この認証では、サービスサーバ4から送信されてきた機器ID、クライアント乱数、サーバ乱数の組から、CE機器3と同じロジックでダイジェストを生成し、サービスサーバ4から送信されてきたダイジェストと一致するか否かをチェックする。

一致した場合、CE機器3は認証され、一致しない場合は認証されない。

そして、認証サーバ5は、認証結果をサービスサーバ4に送信する（ステップ164）。

また、CE機器3のパスフレーズは、機器IDから求める（秘密情報特定手段）。

【0074】

サービスサーバ4は、認証サーバ5から認証結果を受信し（認証結果受信手段）、その認証結果がCE機器3を認証するものであった場合、サービスの提供を開始し（ステップ152）、CE機器3ではそのサービスを利用する（ステップ140）。

なお、ステップ164で認証サーバ5がサービスサーバ4に認証結果を送信する際に、図6のフローチャートと同様にして、認証サーバ5とサービスサーバ4の間でCE機器3の機器情報と保有者情報を確認するように構成することもできる。

【0075】

図9は、ステップ162（図8）のダイジェスト認証処理の手順を説明するためのフローチャートである。

まず、認証サーバ5は、サービスサーバ4から受信した認証情報に含まれる機器IDを用いてCE機器3のパスフレーズを検索して取得する（ステップ174）。なお、認証サーバ5は、予め機器IDとパスフレーズを対応させて記憶している。

【0076】

次に、認証サーバ5は、サービスサーバ4から受信した認証情報に含まれるサーバ乱数とクライアント乱数を取得する（ステップ174）。

次に、認証サーバ5は、ステップ174で検索したパスフレーズと、ステップ174で取得したサーバ乱数及びクライアント乱数を組み合わせ、CE機器3と同じロジックにてこれをハッシュ化し、ダイジェストを生成する（ステップ176）。

【0077】

次に、認証サーバ5は、ステップ176で生成したダイジェストと、サービスサーバ4から受信した認証情報に含まれるダイジェストを比較し、同一であるか否かを判断する（ステップ178）。

ダイジェストが一致する場合（ステップ180；Y）、認証サーバ5は、CE機器3が認証されたものと判断し（ステップ182）、ダイジェストが一致しな

い場合（ステップ180；N）、認証サーバ5は、CE機器3が認証されなかったものと判断する（ステップ154）。

【0078】

図8のフローチャートで示した手順では、図4のフローチャートで示したようなワンタイムID1、ワンタイムID2を用いることなく機器認証を行うことができる。

【0079】

以上に説明した本実施の形態では、以下のような効果を得ることができる。

（1）機器認証モジュール7は、サービスサーバ4が生成したサーバ乱数を用いてパスフレーズをダイジェストに変換した後これを出力するため、第三者が機器認証モジュール7の出力からパスフレーズを読み取ることはできない。

（2）暗号化モジュール8は、機器認証モジュール7からダイジェスト化されたパスフレーズを受信するため、機器認証モジュール7と暗号化モジュール8をスタティックリンクにより結合する必要がある。そのため、機器認証モジュール7と暗号化モジュール8をダイナミックリンクで接続するように構成し、暗号化モジュール8を他のモジュールからも利用できるようにすることができる。

【0080】

（3）暗号化モジュール8は、機器認証モジュール7も含め他のモジュールと共用できるため、暗号化モジュール8を複数用意する必要が無く、CE機器3のシステムの冗長性を解消することができる。そのため、CE機器3のメモリ領域を有効利用することができる。

（4）認証サーバ5とCE機器3で同じロジックにてダイジェストを生成することにより、CE機器3が生成したダイジェストと認証サーバ5が生成したダイジェストの一致を判断することにより機器認証を行うことができる。

（5）パスフレーズそのものではなく、機器認証ごとに値が変化するダイジェストが通信経路で送受信されるため、例えばダイジェストがネットワーク上で第三者に奪取されたとしても、被害を小さい範囲にとどめることができる。即ち、パスフレーズは、機器認証で同じものが何回でも使用できるのに対し、ダイジェストは機器認証ごとに異なるからである。

【0081】

(実施の形態の変形例)

図10は、本実施の形態の変形例を説明するための図である。

図に示したように、本変形例では、機器認証モジュール7を耐タンパチップ35に格納する。

耐タンパチップ35は、集積回路を収納したICチップによって構成された耐タンパ装置であって、改竄や複製、内部の論理構造の解読などの不正行為に対して十分な防御手段を講じてある。

タンパ(tamper)とは、装置を勝手にいじったり手を加えたりするという意味であり、情報などを不正に変更するという意味もある。

【0082】

耐タンパチップ35は、機器IDとパスフレーズ、及び、パスフレーズとサーバ乱数を組み合わせた情報をハッシュ化するハッシュ化機が内蔵された一種のブラックボックスとなっている。

耐タンパチップ35は、耐タンパ仕様で製造されているため、第三者は、耐タンパチップ35を物理的に分解して内部の情報を得ることは困難である。

即ち、耐タンパチップ35を物理的に分解して、秘密情報であるパスフレーズや、ハッシュ化に用いるハッシュ関数を知ることは困難である。

【0083】

また、耐タンパチップ35内のパスフレーズは、サーバ乱数と共にハッシュ化されたダイジェストとして出力されるため、耐タンパチップ35から出力された情報からパスフレーズを解析することも困難である。即ち、ハッシュ関数は一方方向性関数であり、逆変換が困難だからである。

このように、耐タンパチップ35の出力情報から内部の秘密情報を探知することも困難である。

【0084】

図11は、本変形例のハードウェア的な構成の一例を示した図である。

図に示したように、耐タンパチップ35は、バス24に接続しており、CPU21から情報の入出力を行えるようになっている。

即ち、CPU 21は、耐タンパチップ35に対して、サーバ乱数を入力し、耐タンパチップ35から機器IDとダイジェストを受け取ることができる。

【0085】

以上のように、耐タンパチップ35に、パスフレーズ（秘密情報）とハッシュ化機を内蔵し、パスフレーズを出力する際には、ハッシュ化したダイジェストを出力することにより、第三者の手にパスフレーズが渡ることを防ぐことができる。

このように、耐タンパ装置に、秘密情報とこの秘密情報の変換機能を内蔵し、耐タンパ装置から秘密情報が出力される場合は、変換機能で変換された値が出力されるように構成することにより、秘密情報を物理的、及び解析的に探索することが困難になる。そのため、セキュリティレベルを強化することができる。

【0086】

本変形例では、一例として、耐タンパチップ35にパスフレーズとハッシュ化機を内蔵した例について説明したが、この他に、例えば、秘密鍵や共通鍵などの暗号鍵情報を用いるシステムでは、これらの暗号鍵情報と、入力情報に対する署名機能や暗号化機能を耐タンパ装置に内蔵することにより、暗号鍵情報の漏洩を防ぐことができる。

【0087】

【発明の効果】

本発明によれば、端末機器内のメモリを有効利用することができる。

【図面の簡単な説明】

【図1】

本実施の形態の機器認証システムの構成を説明するための図である。

【図2】

CE機器の機器認証に関する構成要素を説明するための図である。

【図3】

CE機器のハードウェア的な構成の一例を示した図である。

【図4】

機器認証を行う手順を説明するためのフローチャートである。

【図 5】

ダイジェスト認証処理の手順を説明するためのフローチャートである。

【図 6】

サービスサーバが認証サーバで認証結果を確認する手順を説明するためのフローチャートである。

【図 7】

C E 機器が認証サーバを確認する別のシーケンスを説明するためのフローチャートである。

【図 8】

機器認証を行う他の手順を説明するためのフローチャートである。

【図 9】

ダイジェスト認証処理の手順を説明するためのフローチャートである。

【図 1 0】

本実施の形態の変形例を説明するための図である。

【図 1 1】

本変形例のハードウェア的な構成の一例を示した図である。

【図 1 2】

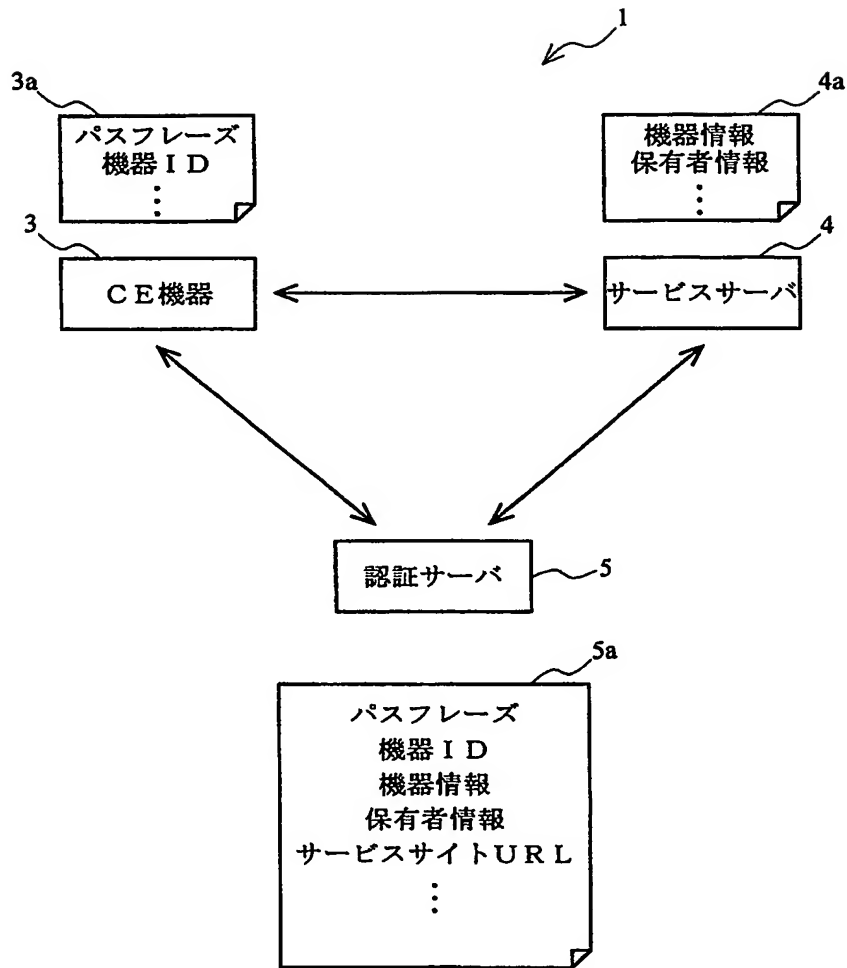
従来の C E 機器の構成を説明するための図である。

【符号の説明】

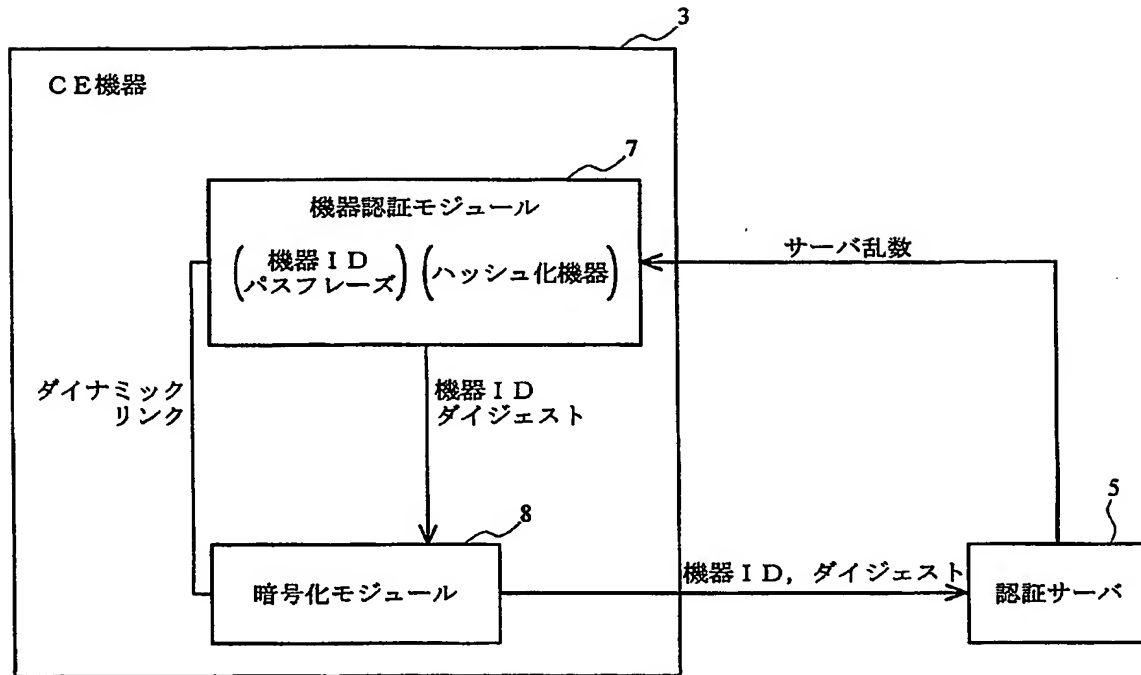
- | | | | |
|-----|-----------|---|----------|
| 1 | 機器認証システム | 3 | C E 機器 |
| 4 | サービスサーバ | 5 | 認証サーバ |
| 7 | 機器認証モジュール | 8 | 暗号化モジュール |
| 3 5 | 耐タンパチップ | | |

【書類名】 図面

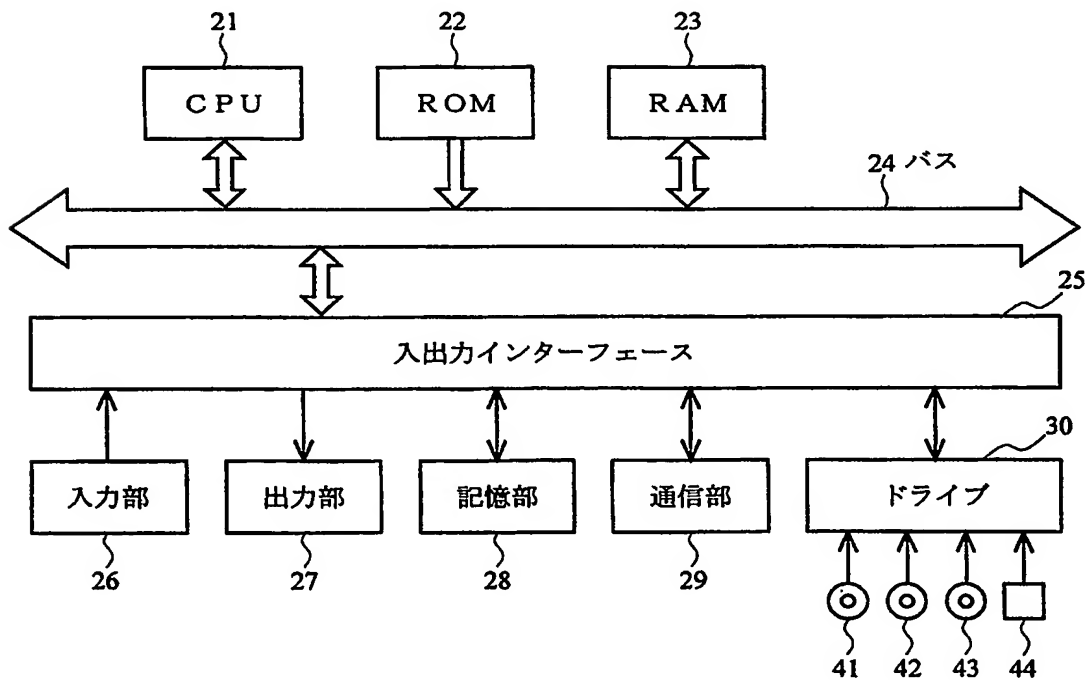
【図 1】



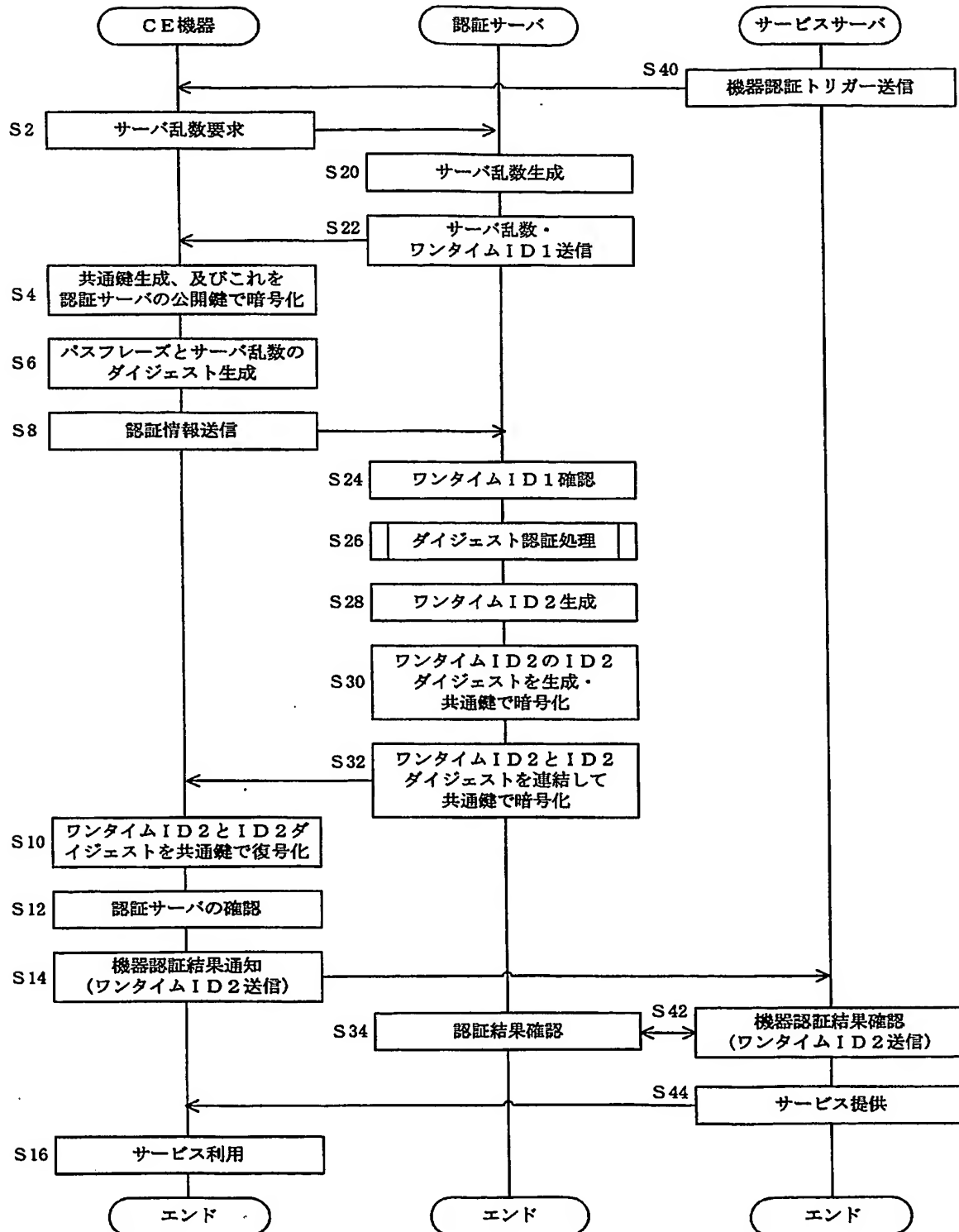
【図 2】



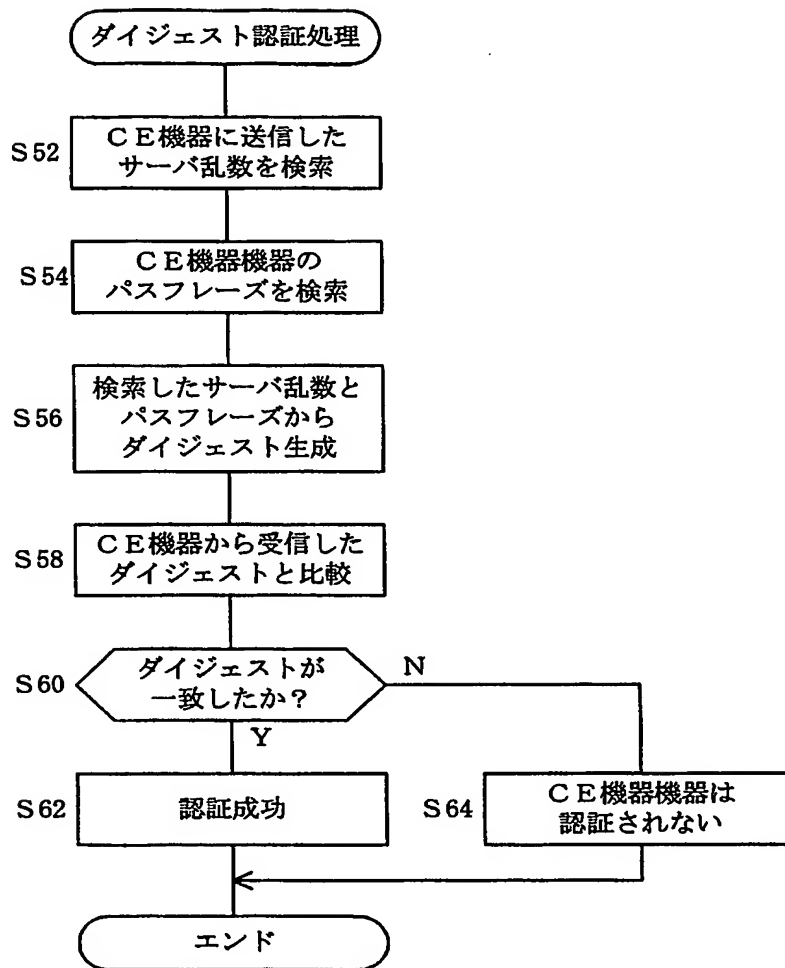
【図 3】



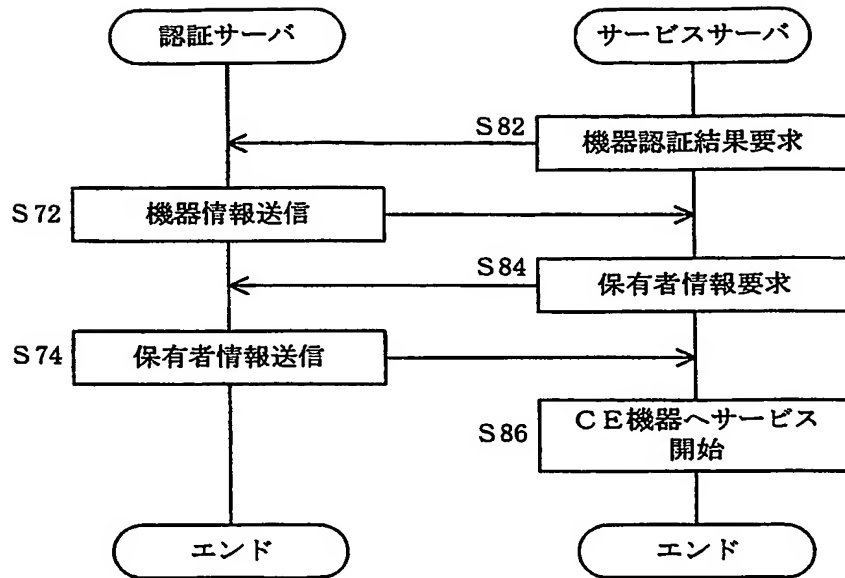
【図 4】



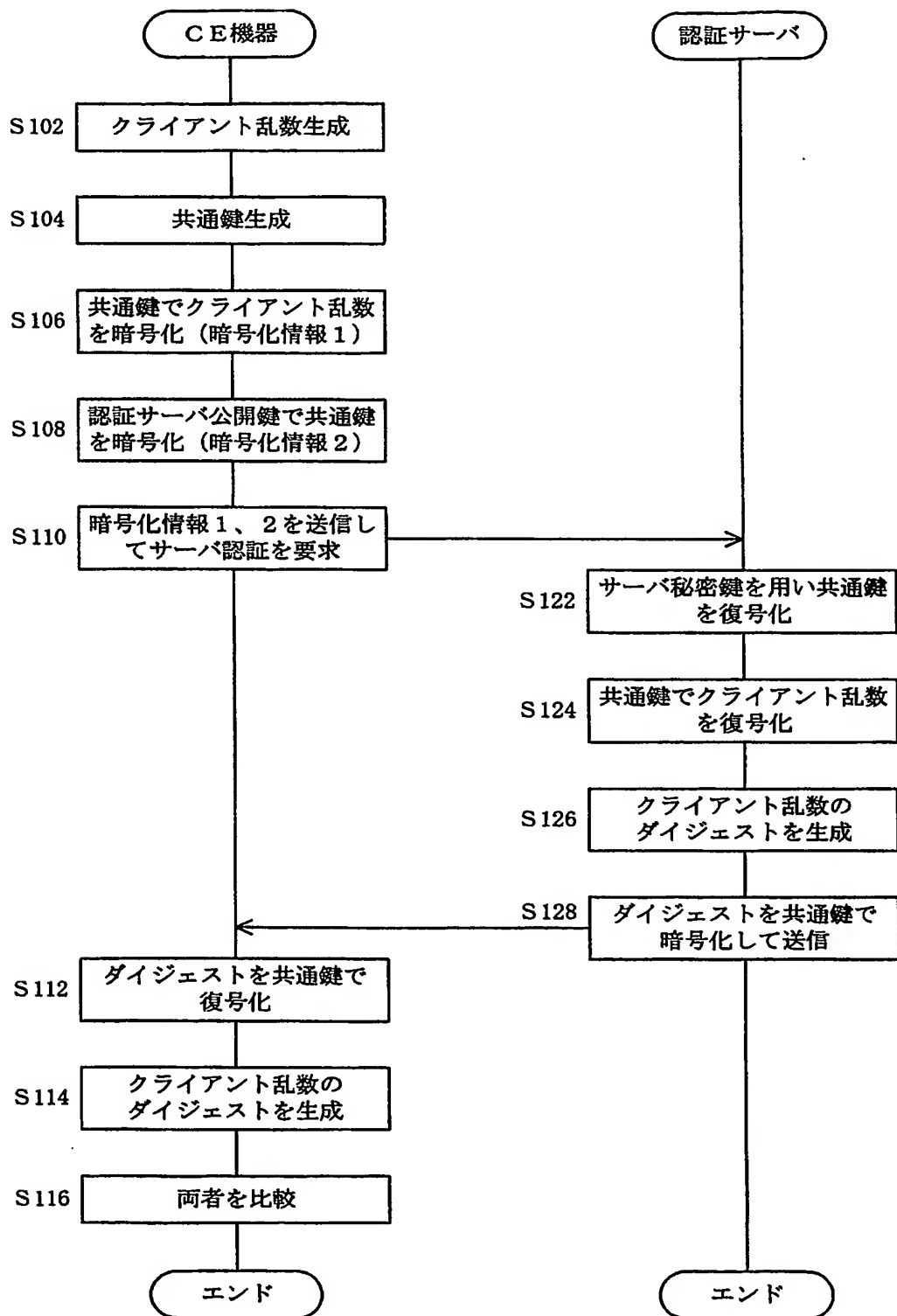
【図 5】



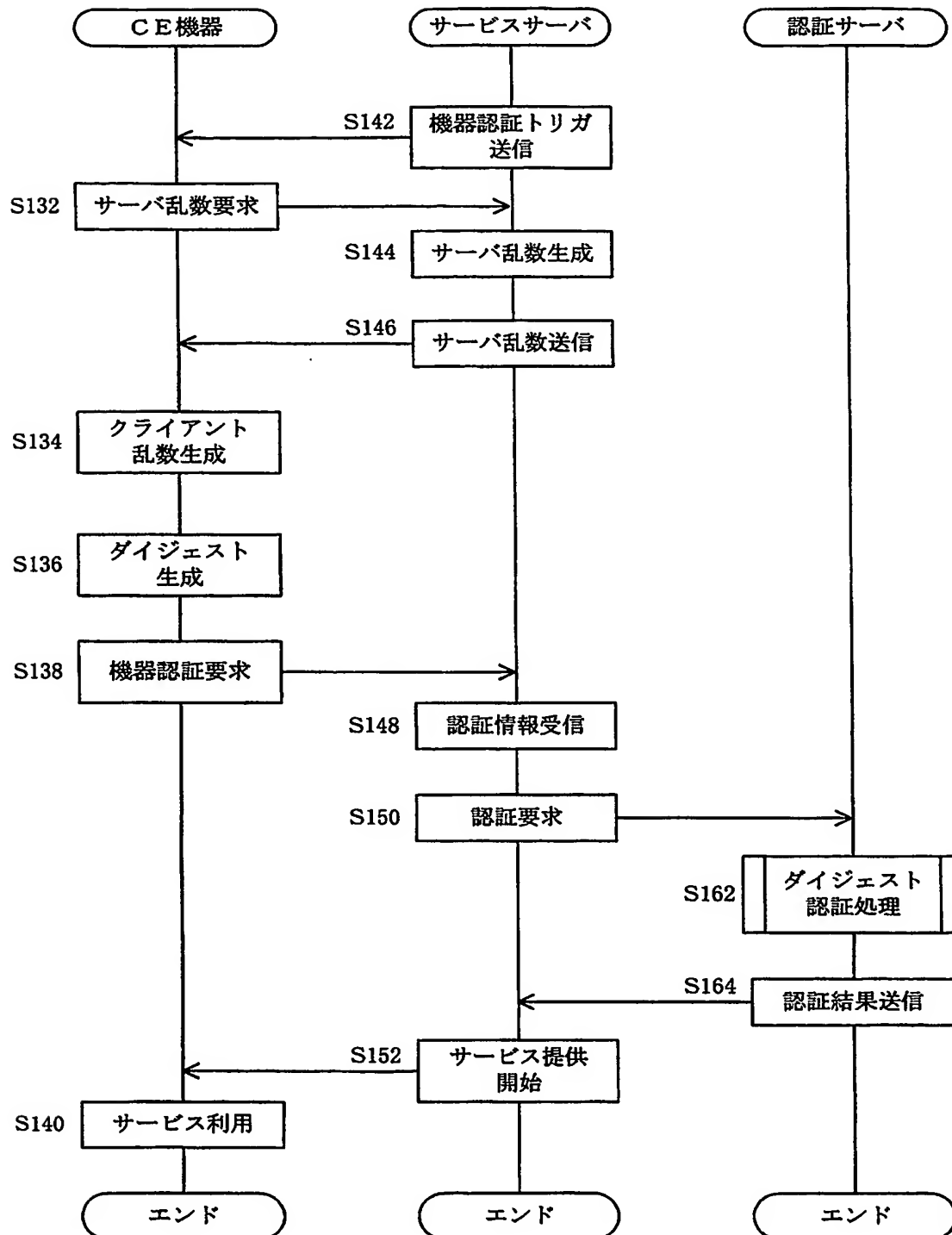
【図 6】



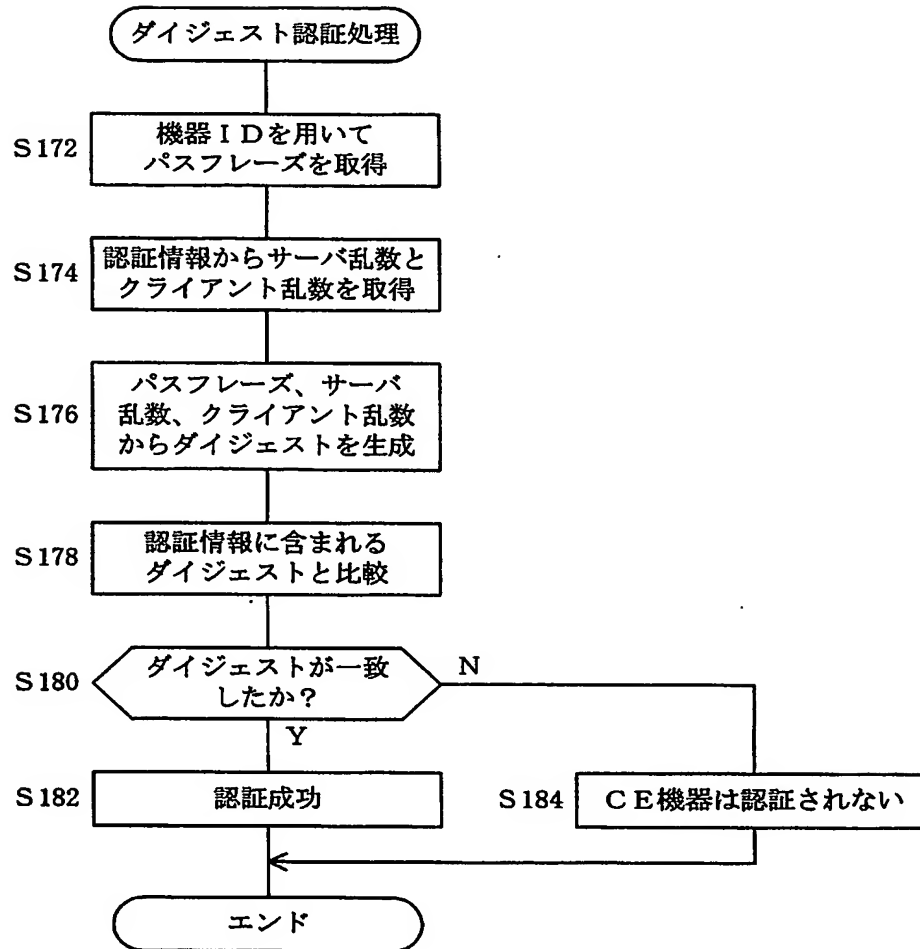
【図7】



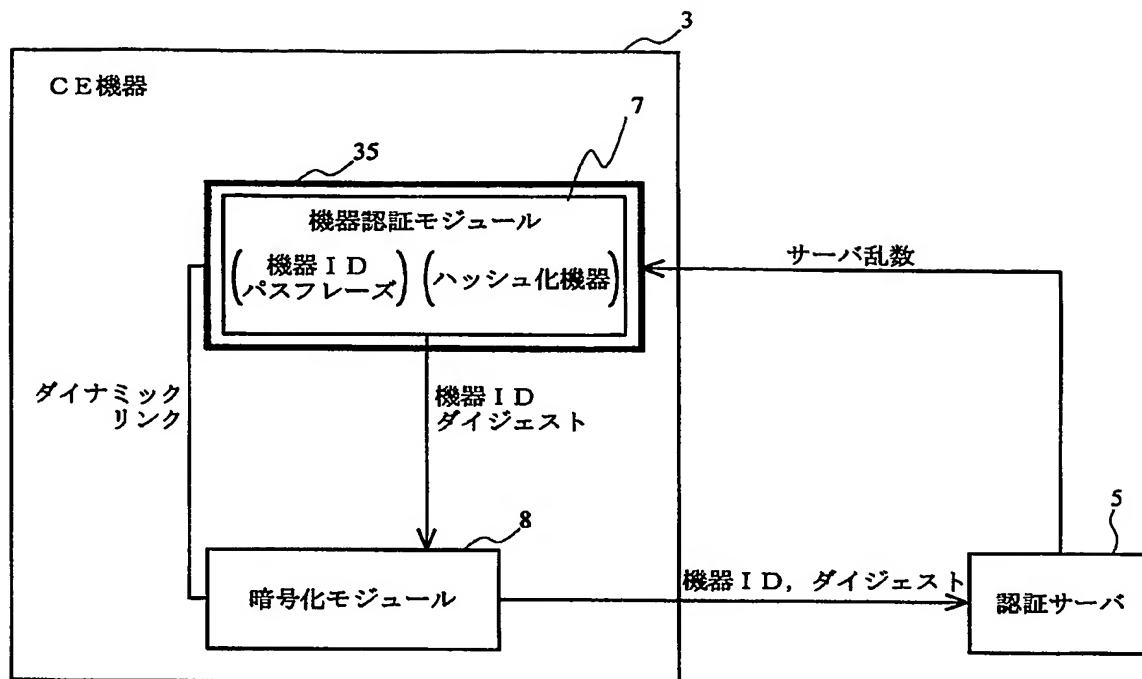
【図 8】



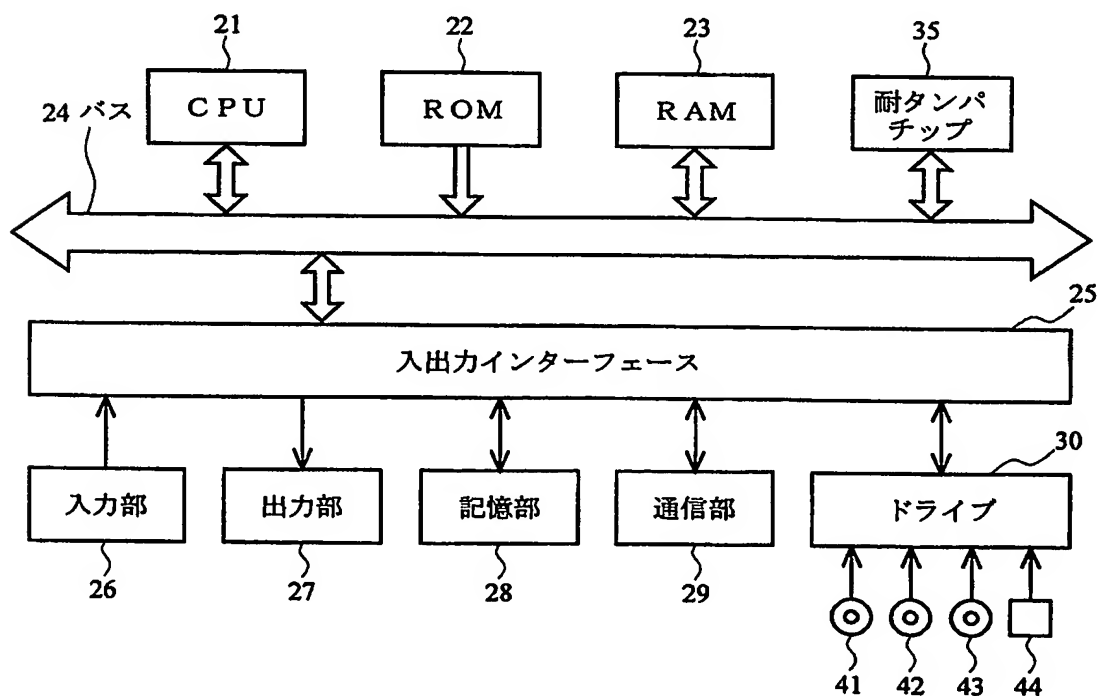
【図 9】



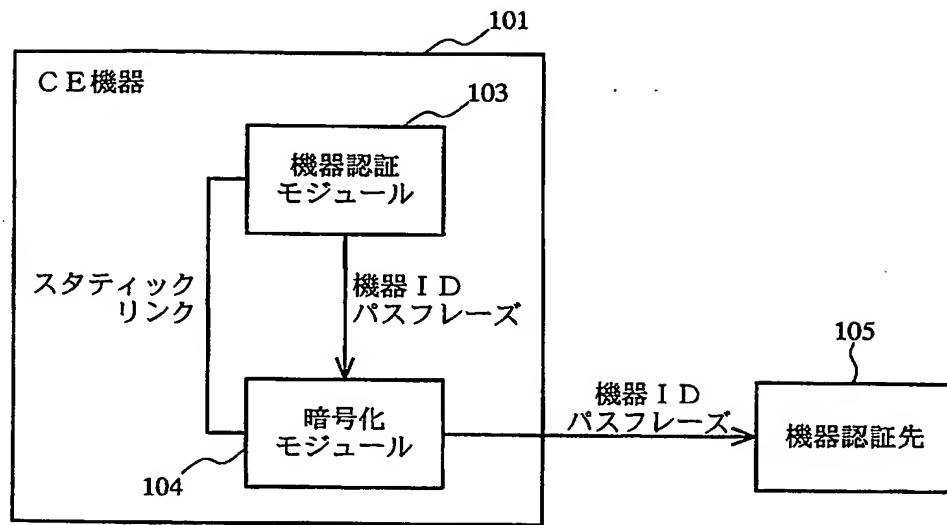
【図 10】



【図 11】



【図 12】



【書類名】 要約書

【要約】

【課題】 CE機器において、機器認証モジュールと暗号化モジュールをダイナミックリンクにて接続できるようにすること。

【解決手段】 認証サーバ5で乱数を発生させる。機器認証モジュール7はパスフレーズとこの乱数を組み合わせてダイジェストを生成し、これと機器IDを暗号化モジュール8に渡す。暗号化モジュールは、通信経路を暗号化し、これらの情報を認証サーバ5に送信する。認証サーバ5は、機器IDからパスフレーズを検索し、これと先に生成した乱数を組み合わせてダイジェストを生成する。このダイジェストと暗号化モジュール8から受信したダイジェストを比較して機器認証を行う。暗号化モジュール8は、機器認証モジュール7からパスフレーズではなくダイジェストを受け取るため、スタティックリンクにて接続せずにダイナミックリンクで接続することができる。

【選択図】 図2

認定・付加情報

特許出願の番号	特願 2003-188141
受付番号	50301092219
書類名	特許願
担当官	第七担当上席 0096
作成日	平成 15 年 7 月 3 日

< 認定情報・付加情報 >

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川 6 丁目 7 番 35 号
【氏名又は名称】	ソニー株式会社

【代理人】

申請人

【識別番号】	100096655
【住所又は居所】	東京都新宿区西新宿 8-12-8 梅屋ビル B1
【氏名又は名称】	川井 隆

【選任した代理人】

【識別番号】	100091225
【住所又は居所】	東京都新宿区西新宿 8-12-8 梅屋ビル B1
【氏名又は名称】	仲野 均

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日

1990年 8月30日

[変更理由]

新規登録

住 所

東京都品川区北品川6丁目7番35号

氏 名

ソニー株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☒ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.